УДК 519.816
DOI: 10.32626/2308-5878.2019-19.168-174

Н. К. Тимофієва, д-р техн. наук
Міжнародний науково-навчальний центр інформаційних технологій та систем НАН та МОН України, м. Київ

КРИТЕРІЇ ПОДІБНОСТІ ДИНАМІЧНИХ ЗАДАЧ КОМБІНАТОРНОЇ ОПТИМІЗАЦІЇ

У комбінаторній оптимізації можна навести багато прикладів, коли задачі з різних класів розв'язуються за однією і тією ж обчислювальною схемою. Це пов'язано з тим що оговореним задачам властива подібність, завдяки якій вони розв'язуються одним методом або модифікацією одного і того ж алгоритму. Вона відрізняється від геометричної та описаної в теорії подібності. Для її встановлення проводиться аналіз задач різних класів з метою виявлення спільних ознак (критеріїв), за якими визначається їхня подібність. Використання цієї властивості дозволяє розробляти однакові методи та алгоритми для їхнього розв'язання. Задачі комбінаторної оптимізації, як правило, подібні за аргументом цільової функції, а задачі з комбінаторики — за способом утворення та впорядкування комбінаторних конфігурацій. Завдяки цій властивості їхні множини генеруються одним і тим же алгоритмом або його модифікацією.

У статті описано ознаки, за якими встановлюється подібність динамічних задач, що відносяться до різних класів. Задачі комбінаторної оптимізації, в яких у процесі їхнього розв'язання генерується поточна інформація, за якою оцінюється результат, а пошук оптимального розв'язку проводиться поетапно з обчисленням часткових сум цільової функції, названо динамічними. Основними ознаками подібності для них є зміна результату розв'язання в часі та для його поточного відліку необхідність обчислення часткової цільової функції. Процес їхнього розв'язання описується орієнтованим ациклічним графом, а часткові значення цільової функції змінюються в часі та обчислюються за рекурентними правилами. При знаходженні їхніх оптимальних значень виконується принцип Беллмана. Виявлені властивості подібності, які характерні для задач цього класу, визначають їхню універсальність, завдяки якій вони розв'язуються одним і тим же методом. Для розв'язання цих задач, як правило, використовують динамічне програмування. Вивчення та використання цієї властивості в комбінаторній оптимізації в подальшому дозволить зводити нерозв'язні задачі до розв'язних. Наведено приклади деяких динамічних задач комбінаторної оптимізації.

Ключові слова: *комбінаторна оптимізація, комбінаторна конфігурація, динамічні задачі комбінаторної оптимізації, подібність задач комбінаторної оптимізації, цільова функція.*

Вступ. Властивість подібності вивчають в геометрії, але вона характерна і для різноманітних фізичних явищ. В комбінаторній оптимізації також має місце подібність, яка пов'язана з тим, що для розв'язання задач різних класів використовують універсальні методи та алгоритми. Для її встановлення необхідно провести аналіз задач комбінаторної оптимізації різних класів та виявити ознаки, за якими вони розв'язуються за однією і тією ж обчислювальною схемою.

Аналіз останніх досліджень та публікацій за темою. В комбінаториці та комбінаторній оптимізації можна навести багато прикладів, коли задачі з різних класів розв'язуються за однією і тією ж обчислювальною схемою, наприклад [1, 2]. Ця властивість в літературі достатньою мірою не висвітлена, хоча існуючі універсальні методи орієнтовані на розв'язання різноманітних таких задач. У роботі [3] наведено деякі ознаки, за якими встановлюється подібність задач в комбінаторній оптимізації, що дає можливість розробляти універсальні методи та алгоритми. Тому однією з проблем у теорії комбінаторної оптимізації є виявлення критеріїв подібності з метою узагальнення та використання для їхнього розв'язання універсальних підходів.

Загальна математична постановка задачі комбінаторної оптимізації. Задачі комбінаторної оптимізації, як правило, задаються на одній або кількох множинах, наприклад $A=\{a_1,...,a_n\}$ та $B=\{b_1,...,b_{\tilde{n}}\}$, елементи яких мають будь-яку природу [4]. Назвемо ці множини *базовими*. Наявні два типи задач. В *першому* типі кожну з цих множин подамо у вигляді графа, вершинами якого є її елементи, а кожному ребру поставлено у відповідність число $c_{lt}\in R$, яке називають вагою ребра (R — множина дійсних чисел); $l\in\{1,...,n\}$, $t\in\{1,...,\tilde{n}\}$, n — кількість елементів множини A, $\tilde{n}$ — кількість елементів множини B. Покладемо, що $n=\tilde{n}$. Між елементами цих множин існують зв'язки, числове значення яких назвемо вагами. Величини $c_{lt}\in R$ — *вхідні* дані, які задамо матрицями. В *другому* типі задач між елементами заданої множини зв'язків не існує, а вагами є числа $v_j\in R$, $j\in\{1,...,n\}$, яким у відповідність поставлено деякі властивості цих елементів, числові значення яких задаються скінченними послідовностями, що також є вхідними даними.

Для обох типів задач із елементів однієї або кількох базових множин утворюється комбінаторна множина W — сукупність комбінаторних конфігурацій певного типу (перестановки, вибірки різних типів, розбиття тощо). На елементах w комбінаторної множини W вводиться цільова функція $F(w)$. Необхідно знайти елемент w^* множини W, для якого $F(w)$ набуває екстремального значення при виконанні заданих обмежень.

За способом обчислення цільової функції виділимо задачі, в яких для певного варіанту розв'язку її значення обчислюється одночасно. Такі задачі назвемо статичними. Задачі, в яких в процесі їхнього розв'язання генерується поточна інформація, за якою оцінюється результат, а пошук оптимального розв'язку проводиться поетапно з обчисленням часткових сум цільової функції, назвемо динамічними.

Для моделювання прикладних задач в рамках теорії комбінаторної оптимізації необхідно:

1) визначити вид задачі (статична або динамічна);
2) визначити базові множини, якими задається певна задача;
3) за вхідними даними визначити її тип;
4) визначити аргумент цільової функції (комбінаторну конфігурацію);
5) змоделювати цільову функцію.

Під комбінаторною конфігурацією розуміємо будь-яку сукупність елементів, яка утворюється з усіх або з деяких елементів заданої базової множини $A = \{a_1, ..., a_n\}$ [6]. Позначимо її впорядкованою множиною $w^k = (w_1^k, ..., w_\eta^k)$, де $\eta \in \{1, ..., n\}$ — кількість елементів у w^k, $W = \{w^k\}_1^q$ — множина комбінаторних конфігурацій. Верхній індекс k ($k \in \{1, ..., q\}$) у w^k позначає порядковий номер w^k у W, q — кількість w^k у W.

Ознаки подібності динамічних задач комбінаторної оптимізації. Основними ознаками подібності для динамічних задач є зміна результату розв'язання в часі та для його поточного відліку обчислення часткової цільової функції. Процес їхнього розв'язання описується орієнтованим ациклічним графом, а часткові значення цільової функції змінюються в часі та обчислюються за рекурентними правилами. При знаходженні оптимального значення часткової цільової функції виконується принцип Беллмана. Аргументом цільової функції в них є вибірки різних типів, а також розбиття n-елементної множини на підмножини. Вони, як правило, розв'язуються одним і тим же методом — динамічним програмуванням.

Динамічні задачі комбінаторної оптимізації. До динамічних задач відносяться такі задачі: сегментація та розпізнавання мовленнєвих сигналів, задача Джонсона з теорії розкладів, задача класифікації, здача збереження довкілля та ін.

Задача Джонсона з теорії розкладів. Найпростіша задача з теорії розкладів (задача Джонсона) формулюється так [2, 5]. Задано n деталей. Кожна з деталей повинна пройти послідовну обробітку на m машинах. Кожна машина також виконує одну операцію. Необхідно скласти такий

розклад обробітку деталей, щоб затрачений на ці операції час був би мінімальний за умови, що він не перевищує заданої величини T.

У цій задачі задано дві множини A і B, між елементами яких існує певна залежність, числові значення якої назвемо вагами. Подамо їх несиметричною матрицею C розмірністю $\tilde{n} \times n$, де величина c_{sl} відповідає значенню часу, який необхідно затратити на обробку l-ї деталі s-ю машиною. Час послідовної обробки всіх n елементів множини A за будь-якого розкладу, який би не перевищував заданої величини T, невідомий, тому спочатку для вибірки із n елементів $a_l \in A$ по n знаходимо перестановку, для якої значення цільової функції — мінімальне і не перевищує величини T. Якщо одержаний розв'язок не задовольняє цій умові, то задача розв'язується для вибірки із n елементів $a_l \in A$ по η. З цього випливає, що аргументом цільової функції в розглянутій задачі є розміщення без повторень, яке утворюється шляхом знаходження сполучення із n елементів по η, для якого генеруються $\eta!$ перестановок, $\eta \in \{1, ..., n\}$.

Для i-го сполучення уведемо комбінаторну матрицю $Q(\mu^i)$ розмірністю $\tilde{n} \times \eta$, в яку входять стовпці матриці C, номера яких збігаються з номерами елементів множини A, з яких утворено сполучення без повторень $\mu^i \in \mathrm{M}$, $i \in \{1, ..., 2^n - 1\}$, M — множина сполучень. Із фіксованої матриці $Q(\mu^{i*})$ утворимо $\eta!$ комбінаторних матриць $Q'(\mu^{i*}, \omega^k)$, які залежать від перестановки $\omega^k = (\omega_1^k, ..., \omega_\eta^k) \in \Omega$, $k \in \{1, ..., \eta!\}$, $\eta \in \{1, ..., n\}$, Ω — множина перестановок. Цільова функція в задачі планування з теорії розкладу набуде вигляду

$$F(\mu^{i*}, \omega^k) = \sum_{l=1}^{\eta} \sum_{s=1}^{\tilde{n}} g_{sl}(\mu^{i*}) + \sum_{l=1}^{\eta-1} \sum_{s=2}^{\tilde{n}} \left| g'_{sl}(\mu^{i*}, \omega^k) - g'_{s-1\,l+1}(\mu^{i*}, \omega^k) \right|, \quad (1)$$

де $\sum_{l=1}^{\eta} \sum_{s=1}^{\tilde{n}} g_{sl}(\mu^{i*})$ — постійна для будь-якої з $\eta!$ перестановок величина, що визначає затрачений час на обробку деталей, який задано за умовою. Вона не залежить від перестановки, а змінюється в залежності від варіанту сполучення μ^i; $\sum_{l=1}^{\eta-1} \sum_{s=2}^{\tilde{n}} \left| g'_{sl}(\mu^{i*}, \omega^k) - g'_{s-1\,l+1}(\mu^{i*}, \omega^k) \right|$ — сумарний час простою машин. Ця величина — змінна і залежить як від варіанту сполучення μ^i так і від перестановки $\omega^k = (\omega_1^k, ..., \omega_\eta^k)$. За виразом (1) визначається сумарне значення цільової функції.

Задача Джонсона полягає у знаходженні таких μ^{i*} і ω^{k*}, для яких значення $F(\mu^{i*}, \omega^{k*})$ було б мінімальним і $F(\mu^{i*}, \omega^{k*}) \le T$. Процес її розв'язання описується орієнтованим ациклічним графом, а часткові значення цільової функції змінюються в часі і обчислюються за рекурентними правилами. При обчисленні часткової цільової функції для неї виконується принцип Беллмана.

Задача розпізнавання мовлення та задача сегментації мовленнєвого сигналу [6]. Задача сегментації мовленнєвих сигналів полягає у виділенні на заданому відрізку вхідного сигналу майже періодичних та неперіодичних ділянок, а в майже періодичних визначаються довжини поточного майже періоду. Розпізнавання мовлення — це процес автоматичної обробки мовленнєвого сигналу з метою визначення послідовності слів, яка передається цим сигналом. Вона полягає у знаходженні для вхідного сигналу найбільш правдоподібного еталону з усіх можливих еталонних сигналів.

Мовленнєвий сигнал передає мовлення людини в якому спостерігаються ділянки майже періодичні, які моделюють голосні та приголосні звуки, та неперіодичні (шумні звуки). Подамо мовленнєвий сигнал дискретною функцією $f(j)|_1^m$, де m — кількість її значень (відліків сигналу) та проведемо його сегментацію на майже періодичні та неперіодичні ділянки, а в майже періодичних визначимо довжини поточного майже періоду.

Відрізок сигналу, що досліджується, розіб'ємо на ділянки довжиною $L \in \{L_{\min}, L_{\min} + \Delta, L_{\min} + 2\Delta, ..., L_{\max}\}$ з наступним визначенням періодичності сусідніх ділянок, $L_{\min}$ — мінімально можлива довжина майже періоду, $L_{\max}$ — максимально можлива довжина майже періоду, Δ — значення приросту майже періоду (визначається експериментально). За еталонний сигнал приймемо попередню ділянку. При розпізнаванні мовлення для вхідного сигналу знаходиться в бібліотеці подібний еталонний сигнал. Оскільки задача сегментації мовленнєвого сигналу та розпізнавання мовлення — динамічні, то їх розв'язують динамічним програмуванням з використанням кореляції функції $f(j)|_1^m$. Ці задачі описуються орієнтованим ациклічним графом, часткові значення цільової функції в ній змінюються в часі та обчислюються за рекурентними правилами. При знаходженні оптимального значення часткової цільової функції виконується принцип Беллмана.

Висновки. Отже, основними ознаками подібності для динамічних задач комбінаторної оптимізації є зміна результату розв'язання в часі та для нього обчислення часткової цільової функції. Процес їх-

нього розв'язання описується орієнтованим ациклічним графом, а часткові значення цільової функції змінюються в часі та обчислюються за рекурентними правилами. При знаходженні оптимального значення часткової цільової функції виконується принцип Беллмана.

Список використаних джерел:

1. Липский В. Комбинаторика для программистов. Пер. с польск. М. : Мир, 1988. 213 с.
2. Сергиенко И. В., Каспшицкая М. Ф. Модели и методы решения на ЭВМ комбинаторных задач оптимизации. Киев : Наук. думка, 1981. 281 с
3. Тимофієва Н. К. Про подібність задач комбінаторної оптимізації та універсальність алгоритмів. *Системні дослідження та інформаційні технології*. 2013. № 4. С. 27–37.
4. Тимофієва Н. К. Теоретико-числові методи розв'язання задач комбінаторної оптимізації. Автореф. дис. ... докт. техн. наук. Ін-т кібернетики ім. В. М. Глушкова НАН України. Київ, 2007. 32 с.
5. Тимофієва Н. К., Гриценко В. И. Розв'язання задачі планування з теорії розкладу методом структурно-алфавітного пошуку та гібридним алгоритмом. *УСиМ.* 2011. № 3 С. 21–36.
6. Винцюк Т. К. Анализ, распознавание и интерпретация речевых сигналов. Киев : Наук. думка, 1987. 262 с.

CRITERIA OF SIMILARITY OF DYNAMIC PROBLEMS OF COMBINATORIAL OPTIMIZATION

In combinatorial optimization, you can cite many examples when the problems from different classes are solved according to the same computational scheme. This is due to the fact that the specified problems have similarities, due to which they are solved by one method or modification of the same algorithm. It differs from geometric and described in the theory of similarity. For its establishment, an analysis of the problems of different classes is conducted in order to identify common features (criteria) that determine their similarity. Using this property allows you to develop the same methods and algorithms for their solution. The problems of combinatorial optimization, as a rule, are similar of the argument of the objective function, and the problems of combinatorics are similar on the creating and arranging of combinatorial configurations. Due to this property, their sets are generated by the same algorithm or it modification.

The article describes the criterias by which the similarity of dynamic problems relating to different classes is established. The problems of combinatorial optimization, in which in the process of their solution, the current information by which the result is evaluated is generated, and the search for an optimal solution is carried out in stages with the calculation of partial amounts of the objective function, is called dynamic. The main criterias of similarity to them is the change in the result of the solution in time and for its current reference, the need to calculate the partial objective function.

The process of their solution is described by a directed acyclic graph, and the partial values of the objective function change over time and are

calculated according to the recurrent rules. When finding their optimal values, the Bellman principle is followed. The revealed properties of similarity, which are characteristic of the problems of this class, determine their universality, through which they are solved by the same method. Typically, dynamic programming is used to solve these problems. The study and use of this property in combinatorial optimization in the future will allow solving insoluble problems for solvable ones. Examples of some dynamic combinatorial optimization problems are given.

Key words: *combinatorial optimization, combinatorial configuration, dynamic combinatorial optimization problems, similarity of combinatorial optimization problems, objective function.*

Одержано 24.01.2019

УДК 519.1,514.128
DOI: 10.32626/2308-5878.2019-19.174-180

В. О. Устименко*,**, д-р фіз.-мат. наук, професор,
О. С. Пустовіт**

*Університет Марії Кюрі-Склодовської, м. Люблін, Республіка Польща,
**Інститут телекомунікацій і глобального інформаційного простору НАН України, м. Київ

ПРО НОВІ ПОТОКОВІ АЛГОРИТМИ СТВОРЕННЯ ДАЙДЖЕСТІВ ЕЛЕКТРОННИХ ДОКУМЕНТІВ З ВИСОКОРІВНЕВИМ АВАЛАНЧ ЕФЕКТОМ

Пропонується родина залежних від ключа швидких алгоритмів створення дайджестів електронних документів Комп'ютерна симуляція дозволяє дослідити високий рівень аваланч ефекту, що виникає. Нехай K — вільно обране скінчене комутативне кільце, m — додатне ціле число. Алгоритми використовують нещодавно знайдені гомоморфні відображення компресії функцій вільної напівгрупи потенційно нескінчених текстів у алфавіті K на скінчену групу кубічних поліноміальних перетворень m вимірного афінного простору K_m.

Криптографічна стабільність функцій хешування пов'язується зі складними алгебраїчними проблемами, такими як дослідження систем алгебраїчних рівнянь великої степені та задача розкладу нелінійного відображення вільного модуля за заданими твірними.

Для пришвидшення алгоритму дайджестом слова $p = (p_1, p_2, ..., p_n)$, $p_i \in K$ вважатимемо не саме кубічне перетворення $F = \psi(p)$, але його значення $F(w(p))$ на деякому за-

